## CLAIMS

We claim:

1. A method of enciphering information constituted by a finite sequence $\{S_1,S_2,\ldots,S_N\}$ of N symbols $\{S_1,S_2,\ldots,S_N\}$ selected from an alphabet A, wherein there are defined both a secret convention (K) of $\underline{p}$ key symbols $K_1,\ldots,K_p$ selected from a second alphabet B, and a multivariate function M having m+1 variables (m<=N): $M(X_{i1},\ldots,X_{im},Y)$ operating $A^m \times B$ in A, $\{i_1,\ldots,i_m\}$ being $\underline{m}$ distinct indices in the range [1,N] and the function M being objective relative to at least one $(X_{i1})$ of the $\underline{m}$ variables of A, said enciphering method comprising:

initially placing the N symbols $(S_1,S_2,\ldots,S_N)$ constituting the information to be enciphered in the N positions of a shift register, and then

performing a succession of X turns of the shift register implementing a succession of X permutations on the sequences $\{S_1,S_2,\ldots,S_N\}$ such that where $\{S_1,S_2,\ldots,S_N\}$ is the sequence prior to the $j^{th}$ permutation, the sequence after the $j^{th}$ permutation is $\{S_2,S_3,\ldots,S_N,Zj\}$, where Zj is equal to $M(S_{i1},\ldots,S_{im},K_j)$, the enciphered information being constituted by the sequence $\{S'_1,S'_2,\ldots,S'_N\}$ contained in the shift register at the end of the $X^{th}$ permutation resulting from the $X^{th}$ turn of the shift register.

2. An enciphering method according to claim 1, wherein the function $M(X_{i1},\ldots,X_{im},Y)$ is objective relative to the first variable $(X_{i1})$.

3. An enciphering method according to claim 1, wherein the number $\underline{m}$ is equal to N.

4. An enciphering method according to claim 1, wherein the number $\underline{m}$ is less than N.

5. An enciphering method according to claim 1, wherein the number X of permutations is greater than several times the length N of the sequences $\{S_1,S_2,\ldots,S_N\}$.

6. An enciphering method according to claim 5, wherein the number $\underline{m}$ is equal to 3, the function M being defined by $M(X_1,X_2,X_N,Y)$.

7. An enciphering method according to claim 6, wherein the function $M(X_1,X_2,X_N,Y)$ is calculated using the following steps:

$U=t1(X_1,X_N)$

$V=t2(U,Y)$

$Z=t1(V,X_2)$

t1 and t2 being the functions associated with two Latin squares T1 and T2 of size equal to the number N.

8. A method of deciphering information enciphered using the enciphering method of claim 7, wherein the symbols $(S'_1,S'_2,\ldots,S'_N)$ of the sequence $\{S'_1,S'_2,\ldots,S'_N\}$ constituting the enciphered information are reverse symbol by symbol $(S'_N,S'_{N-1},\ldots,S'_1)$, $M(S_1,S_2,S_N,K_j)=Zj$ is calculated using a key symbol Kj beginning with the last key symbol to be used during enciphering, and so on in decreasing order ...Zj,Zj-1,..., with $M(X_1,X_2,X_N,Y)=Z$ being calculated using the following steps:

$V=t1^{*\square}(X_1,X_N)$

$U=t2^{*\square}(V,Y)$

$Z=t1^{*\square}(U,X_2)$

the sequence obtained at the end of the $X^{th}$ permutation reconstituting the information in the clear $\{S_1,S_2,\ldots,S_N\}$.